Cassandra Crossing/ Captatori e Trojan

(449) Cosa sono, cosa non sono, cosa forse dovrebbero essere.

Cassandra Crossing/ Captatori e Trojan

(449) Cosa sono, cosa non sono, cosa forse dovrebbero essere.

9 marzo 2020—Perché parlare sempre di chi è intercettabile e chi no , e non parlare mai dei mezzi delle intercettazioni?
Lasciamo perdere per una volta il pur importante "chi" ed interroghiamoci sull'ancora più importante "come".

Cosa è un trojan?

In tempi antichi, quando i computer stavano solo sulle scrivanie e non avevano anche occhi ed orecchie, erano dei programmi maligni, virus informatici che non potevano propagarsi da soli, ma che avevano bisogno di essere lanciati, anche per una sola volta, dall'utente del computer.
Dei virus informatici senza la capacità di riprodursi da soli, insomma.
Cosa potevano fare?
In linea di massima, qualsiasi cosa potesse fare l'utente del computer, da cancellare tutti i file fino ad intercettare e trasmettere ogni mail ed ogni carattere battuto sulla tastiera.

Oggi sono più pericolosi di ieri?

In un certo senso no, è il mondo che è diventato un posto molto più pericoloso, popolato da persone che hanno permanentemente un computer in tasca, dotato di occhi, orecchie, sensori e tanto altro, persone che su questo computer tengono una parte consistente, e talora prevalente, della propria vita.

Ecco che un trojan, una volta "strumento" potente ma dai pochi e limitati impieghi, è diventato un'arma di distruzione di massa.
Distruzione della privacy, distruzione dei dati, distruzione talvolta della vita fisica.
E di una vera arma si tratta, visto che viene usata come tale, sia in paesi diversamente democratici sia, ahimè, in paesi cosiddetti di democrazia compiuta.

Cosa può fare un trojan che, ipotizziamo, abbia infettato il vostro cellulare?
Può controllarvi, ascoltare le vostre telefonate e farne al vostro posto, vedere con le numerose telecamere, copiare qualsiasi contenuto, SMS, mail, MMS, foto, video, documenti.
Ah, e può ovviamente inserire nuovi contenuti, applicazioni e file di qualunque tipo.
Può usare i numerosi sensori per sapere la vostra posizione esatta usando i dati del ricevitore GPS, ma anche i dati di cella GSM, la bussola, le reti WiFi

raggiungibili, e sapere monto [molto] su cosa sta facendo il vostro corpo usando i dati dell'accelerometro tridimensionale.

Tutte cose evidentemente interessanti per molti, visto il proliferare di aziende informatiche "specializzate" e gli alti prezzi delle licenze d'uso di questi software "borderline", assai tendenti allo "scuro". Sviluppati anche in Italia.

Cosa è invece un captatore informatico?
Nessuno lo sa con esattezza, essendo per ora un concetto legal-informatico in rapida e contrastata evoluzione.

Tentando di riassumere, dovrebbe essere un software in grado di compiere, per via informatica o nel mondo digitale, quelle attività di indagine, ormai ben consolidate e comprese nel mondo analogico.

Quindi:

- [Dovrebbe permettere di fare un pedinamento informatico, se così ordinato dall'autorità giudiziaria, per il periodo autorizzato.]
- [Dovrebbe permettere di eseguire un sequestro informatico.]
- [Dovrebbe permettere di eseguire un'intercettazione ambientale.]
- [Dovrebbe permettere di eseguire un'intercettazione telefonica.]
- [Dovrebbe permettere di eseguire un'intercettazione di corrispondenza elettronica.]

Auspicabilmente, per una data indagine, dovrebbe permettere di fare solo le operazioni decise dall'autorità giudiziaria, con la massima efficienza e senza permettere sconfinamenti.
Dovrebbe anche fornire prova inalterabile di quanto, da chi e quando fatto.

File di log, chiavi crittografiche e marche temporali sono ormai strumenti di uso quotidiano non solo da parte di privati (consapevoli o meno di utilizzarli) ma anche nelle pubbliche amministrazioni, essendo ormai parte integrante dei normali sistemi informatici critici.

Certamente aziende in grado di produrre trojan potrebbero, in via ipotetica, dotarli anche di queste caratteristiche, ormai normali nelle applicazioni, in modo da renderli potenti ma controllabili, rispettosi delle leggi e degni di essere utilizzati in paesi a democrazia compiuta.

Purtroppo i captatori informatici, dotati delle desiderabili caratteristiche sopraelencate, semplicemente non esistono.

Dove si trovano infatti i requisiti tecnici che questi software devono possedere?

La riforma approvata da pochi giorni, che regolamenta solo l'uso del microfono sui dispositivi mobili e non le altre tipologie di intercettazioni, rimanda tutte le questioni ed i requisiti tecnici ad un decreto ministeriale.
Questo è normale nella legislazione italiana, ma ovviamente quello dell'ultima riforma non ha ancora visto la luce.

Per avere un'idea dei requisiti previsti per i captatori, dobbiamo quindi dare un'occhiata all'analogo decreto ministeriale della precedente riforma, varata nel giugno 2017, che è stato pubblicato nel maggio 2018.

Da una rapida occhiata, possiamo constatare che la definizione delle caratteristiche tecniche dei captatori è lunga 200 parole, dedicate solo ad un elenco qualitativo di ciò che i captatori devono fare.

Nella realtà e sul mercato, oggi sono reperibili solo software nati per altri scopi, vere e proprie armi informatiche, trojan onnipotenti dotati di capacità di infezione, inoculazione e gestione sempre più sofisticate, utilizzabili contemporaneamente su grandi quantità di bersagli.

Questi software, essendo appunto armi, sono progettati per massimizzare le loro capacità offensive, e ben poco si curano di ogni altra caratteristica o requisito.

E, ad oggi, **sono gli unici software utilizzabili come captatori informatici**.

By Marco A. L. Calamari on April 6, 2020.

Canonical link

Exported from Medium on January 2, 2024.